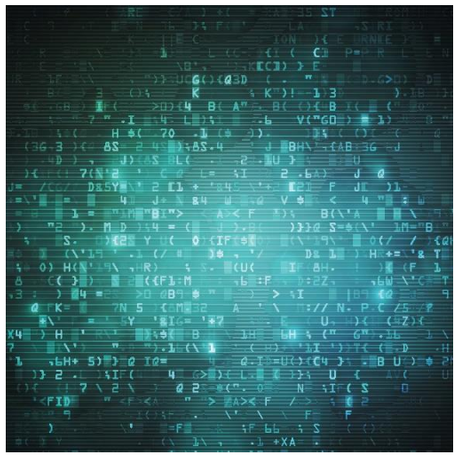
AgilePQ™
Agile Post-Quantum Solutions

Introducing AgilePQ DCM (Digital Conversion Module)

—Next Generation Data Security and Transmission for SCADA Environments

January 6, 2017



AgilePQ™
Agile Post-Quantum Solutions

Today…

Summary of feedback from dozens of one-on-one interviews with energy and water executives in the area of cybersecurity

Overview of AgilePQ DCM capability

Goals for the session:

PROVIDE AN OVERVIEW

GAIN FEEDBACK

AgilePQ™ Agile Post-Quantum Solutions

Current Environment – What we have heard…

Rate of attack on Energy systems from hostile and sophisticated adversaries is growing exponentially

Responsibility for protecting the grid is not well-defined: who is responsible for what?

Who can address and who should address these threats?

Where are the lines for:

Federal or state/local responsibility?	Boards or regulatory direction?
Public or private responsibility?	Grid or internet of things systems?

What measures can proceed now for reasonable cost and in a reasonable timeframe?

AgilePQ™ Agile Post-Quantum Solutions

The Challenge: Grid Systems are Vulnerable to Cyber Attack

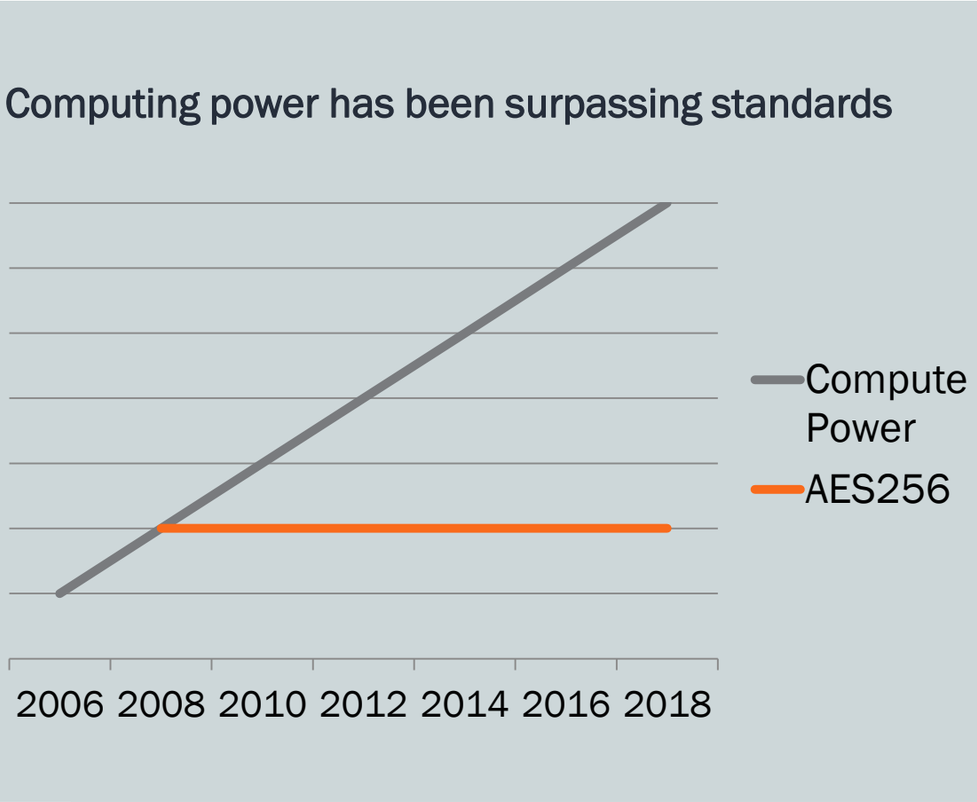
- **AES** (Advanced Encryption Standard) is failing in the wake of expanding computing power and hack attempts. It's footprint is also too large to fit on endpoints.
  - All of these factors put utilities at increasing risk

2010: **80k**

2014: **10M**

2016: **300M**

The # of Hack Attempts in the US Per Day



AgilePQ™
Agile Post-Quantum Solutions

Specific Energy Issues – What is Most Important?

Secure data from sensors throughout the core ICS systems

Secure and authenticate commands sent to SCADA or other ICS

Maintain secure operations in the necessary real time environment (minimize time delays for encryption)

Identify devices attached to SCADA systems and to the grid

Secure customer data

Minimize power draw on remote sensing devices

Justify costs to federal and state regulators

Assure encryption does not hinder recovery speed/resilience

AgilePQ Origins

Company Incorporated in Delaware 2014

Mission: Agile Post-Quantum (APQ) protects and accelerates data communications across IoT, Cloud, SCADA, and Government environments.

Genesis: Improving Communications Link with UAV's using Optimized Code Table Signaling

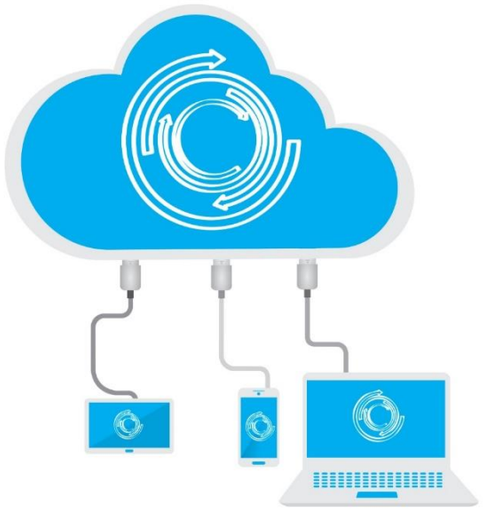
Principal Inventor: Bruce Conway, Co-Founder AgilePQ

Retired Air Force Colonel	Electrical Engineer
Star Wars Program	Specialization in Military Communications

AgilePQ Patents: 4 Issued, 1 allowed, 4 Pending, 2 International PCT Applications

What we do…

AgilePQ DCM systemically authorizes, authenticates, accelerates, and improves efficiency while increasing security of data transmission across IoT, Cloud, SCADA, and Government Environments.



What's in the Name…

Idea for Agile Post-Quantum (AgilePQ) came from world-leading cryptographer, Dr. Taher Elgamal.

Agility in reference to the key size; Post-Quantum in reference to the factorial key search space.

AgilePQ patented methodologies differentiate technology in code theory vs. number theory

> **Three Words Describe Your Company…**
>
> "Agile Post-Quantum"
>
> Dr. Taher Elgamal

AgilePQ DCM Overview

A new solutions that exponentially enhances cybersecurity in SCADA networks from Endpoint to Data Center using DCM (Digital Conversion Module). We give energy and water companies the ability to secure what has been previously un-securable. DCM can secure things previously unprotected, replace AES, or run alongside it to put the power of protection in your hands.

Key Features:

- *Exponentially More Secure than AES 256*

  Small footprint as little as 2.5kb to be able to fit on sensors

  Tuneable Security Levels to align with corresponding degree of risk

  Requires 50-80% less power than current AES

  System Agnostic

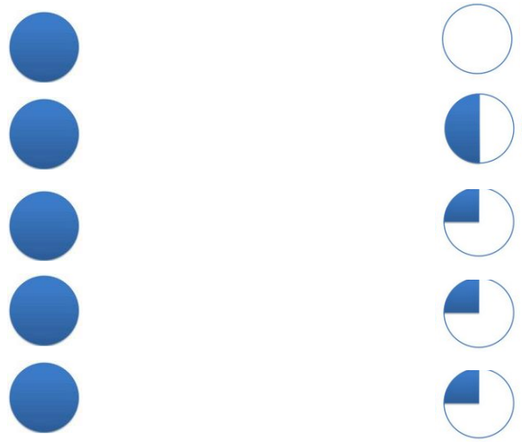
  Installed as Software, Firmware, or Hardware

DCM Closes the Door on 85% of SCADA Vulnerabilities

DCM uniquely addresses 85% of the Vulnerability Risks identified in the R*elative Frequency of NSTB Observed Vulnerabilities published in September 2011 Vulnerability Analysis of Energy Delivery Control Systems by Idaho National Laboratory. The remaining 15% of vulnerabilities involve human behavior*

VULNERABILITIES (% of Total Vulnerabilities):

- Communication Endpoint (43%)
- Communication Channel (16%)
- SCADA Network Access Control (11%)
- Authorization (8%)
- SCADA Authentication (7%)



We provide data security between the Communication Server and all points below it. We secure the pipe to prevent outside intruders.

Statistics are the Percentage of NSTH assessment findings by vulnerability type.

AgilePQ™ Agile Post-Quantum Solutions

Significantly Stronger than AES 256

Current encryption operates in a numbers based world where security is dependent on mathematical equations. DCM functions in a code theory framework that yields exponentially larger search spaces than encryption. Extremely difficult to break

Current Encryption

Number Theory (10^{38})

DCM

Coding Theory (10^{506})

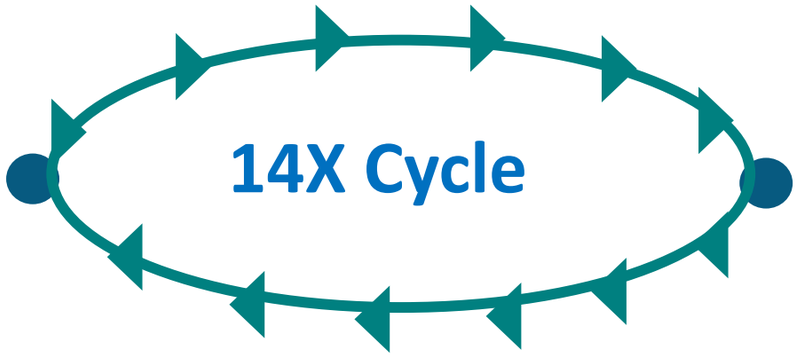
AgilePQ™ Agile Post-Quantum Solutions

DCM Takes Less Time and Draws Less Power than AES 256

- Current encryption requires 14 cycles to obfuscate. DCM completes the process in a single pass
- It also uses a one-time pad making rear view code recognition impossible

Current Encryption

14 Cycles Uses More Power



DCM

A single pass is far more efficient

AgilePQ
Agile Post-Quantum Solutions

Speed and Energy Savings

Key Search Space:

- Orders of Magnitude Greater than AES

Speed:

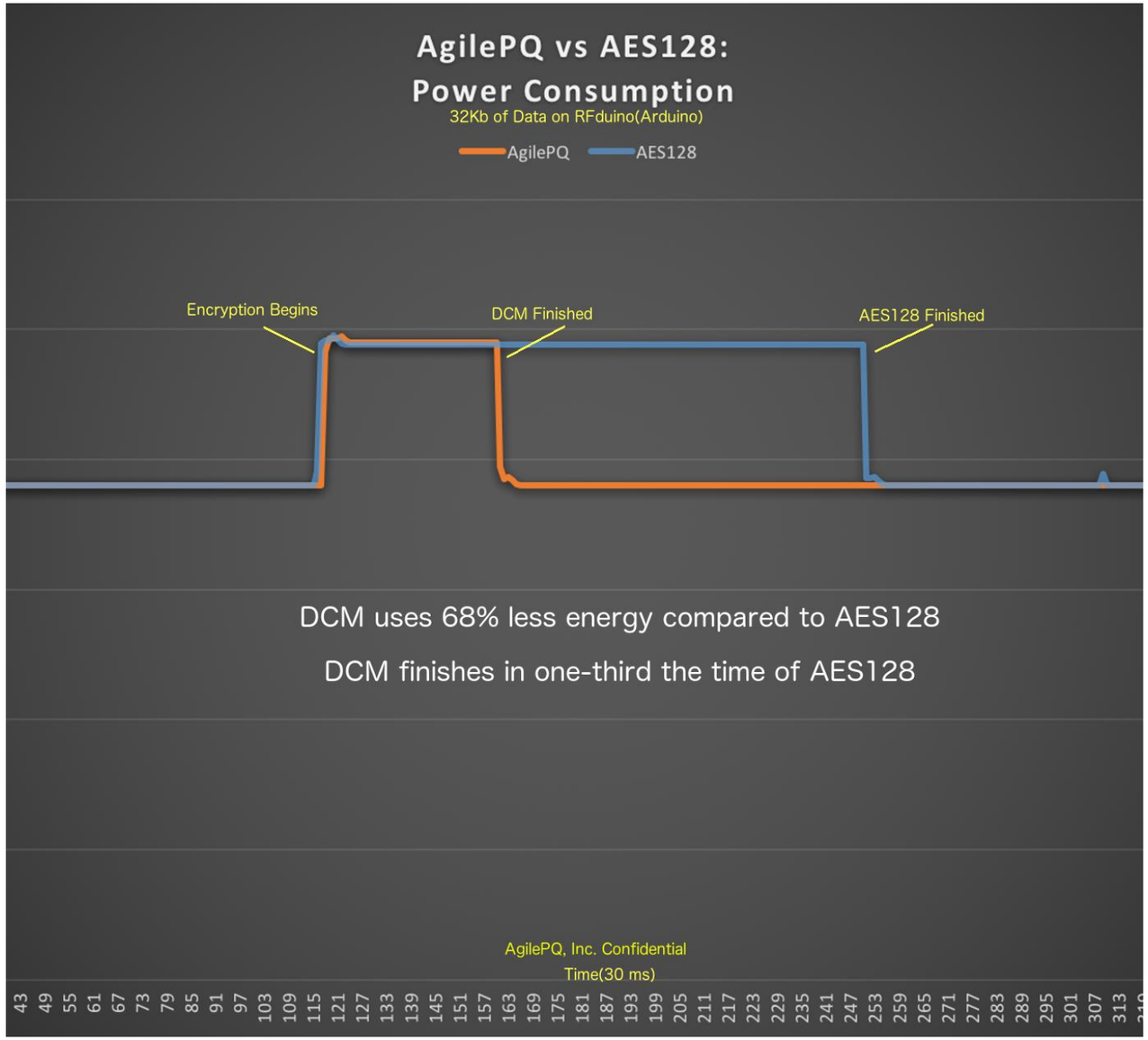
- Faster than HW accelerated AES in all CPU's

Power:

- Consumes 50% - 88% less energy than AES

Size:

- 2.0kB Dynamic RAM
- 2.5kB Flash footprint



AgilePQ
Agile Post-Quantum Solutions

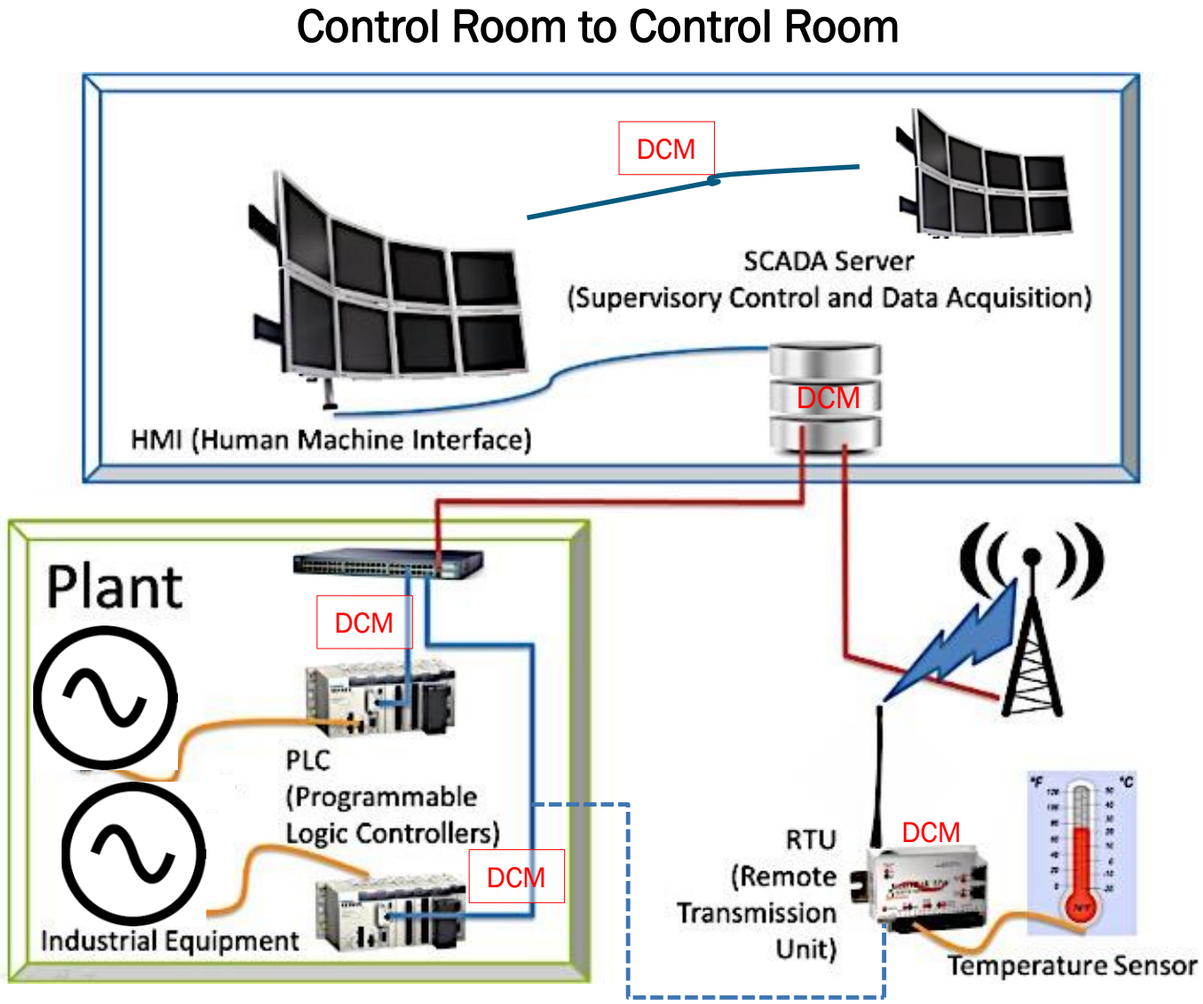
AgilePQ DCM For SCADA

Flexible deployment

- PLC: As Bump-in-the-Wire where PLC has no traditional compute stack
- RTU: As Bump-in-the-Wire or loaded directly on processor
- Control Center: Loaded directly

Flexible Key Size:

- Tailored to implementation environment



AgilePQ™
Agile Post-Quantum Solutions

Implementation

- DCM Elements Auto-configure for secure communication
  - Element self-realizes both client and network sides, announces itself, and is ready for secure data transmission
- DCM provides high security with a flexible key size that can be tailored to any environment
  - DCM can be set up for a small fixed-block message sizes (e.g. much less than typical 16 byte minimum blocks)
  - Or - DCM can be set up for serial data streams
  - All implementations use one-time-pad key solution
- DCM Tables (or ‘keys’) are self-generated, used once, and discarded

Validations and Proofs of Concept

AgilePQ™ Agile Post-Quantum Solutions

Independent Validations

- **Keysight Technologies:** Validated capabilities with independent verification
- **Ponemon Institute:** Engaged US nuclear security experts to attack. No successful compromise
- **University of New South Wales:** 32 million packets no collisions
- **University California San Diego:** Mathematical assessment. "Attack surface is so large virtually impossible to break." Quantum resistant (Search space = 10^{506} vs. 10^{38} for AES 128)

Proof of Concept

- **Innovation lab of a top global networking company (not yet able to name them):** Vetted through their lab and now operating on their routers
- **University of Nebraska Omaha:** Validation of performance on SCADA test bed
- **National Lab SCADA Test:** Soon to undertake validation on national SCADA test bed
- **Microsoft Azure** – Directly connecting newly secured sensors directly to the cloud

SUMMARY OF BENEFITS

DCM offers a unique opportunity to easily and efficiently strengthen the cybersecurity environments of energy providers

FEATURE HIGHLIGHTS:

- Quantum resistant encryption (Search space = 10^{506} vs. 10^{38} for AES 128)
- Small footprint of as little as 2.5kb enables security for entire ecosystem from endpoint/sensor through data center
- Tuneable security levels balancing security vs. power objectives
- 50% - 70% less power consumed than current encryption
- Vetted by the World's elite cryptologists, Keysight Technologies, the Innovation Lab of a global networking company, SCADA Test Bed, Red-Hat Assault Teams, UCSD Cryptology Mathematics PhD, and Microsoft Azure

AgilePQ™
Agile Post-Quantum Solutions

Where would you apply advanced encryption today?

AgilePQ™
Agile Post-Quantum Solutions